REMARKS

In response to the Office Action mailed on October 18, 2007, Applicant respectfully requests reconsideration.

Claims 1-8, 11-21, 23-25 and 27-43 are now pending in this Application.

In this Amendment, claims 1, 18, 21, 38, 39 and 42 have been amended, claims 40 and 41 have been cancelled and claims 44-45 have been added.

Claims 1, 18, 21, 38, 39, 42 and 44 are independent claims and the remaining claims are dependent claims.

Applicant(s) believe that the claim(s) as presented are in condition for allowance. A notice to this affect is respectfully requested.

Claims 21 and 42 have been rejected as nonstatutory under **35 U.S.C. §101**. Accordingly, claims 21 and 42 have been amended to recite instructions that, when executed by a processor responsive to the instructions, perform steps.

The Office Action notes various informalities under **35 U.S.C. §112**. Applicant thanks the Examiner for these observations. The informalities have been amended above.

Claims 1-8, 11-21, 23-25 and 27-43 have been rejected under **35 U.S.C. §103(a)** as being obvious over Krack, U.S. Patent No. 6,941,369 (Krack '369) in view of Balasubramaniyan et al., Comp. Security App. Conf. Proc, (Balasubramaniyan) and Gangadharan et al. IEEE Conf. On Computer Networks and Mobile Computing (Gangadharan).

In particular, the Office Action rejects the claimed elements including "determining an IPC intercept...", "identifying a common access point..." and establishing an IPC intercept....". Gangadharan, however, teaches a 3 tiered mechanism for intrusion control (p. 327, table 2; col. 2, 1st paragraph), outlining micro-firewalls, policy managers, and gateway firewalls. Further, Gangadharan does not disclose a single discrete interception point at which intrusion attempts are funneled and directed to a single, common intrusion mechanism. This is further evidenced by the focus on security policy updates (section 4, pp. 329-330). Since each security "tier" operates independently, Gangadharan suggests value in ensuring that each tier

enforces the same policy. In contrast, in the claimed invention, security intrusions are directed from the interception point and funneled to common intrusion processing (i.e. the data security device), thus mitigating the need for coordinating a security policy among multiple entities.

While the cited portion of Gangadharan addresses an inter-host intrusion from behind the gateway firewall, the Gangadharan approach processes the intrusion at the detecting entity, regardless of the security tier. Gangadharan is then concerned with propagating the updated security policy to other security entities (i.e. the policy manager, in the cited portion). Thus, Gangadharan exhibits an entirely different architecture by distributing the security processing to multiple entities (i.e. in each tier), each operable to handle the intrusion. In contrast, the claimed invention funnels the attempts to a common entity operable to centralize intrusion processing. Accordingly, Gangadharan teaches away from the claimed invention by disclosing DISTRIBUTED processing of detected intrusions, while the claimed approach CENTRALIZES intrusion processing. Communication between the security entities (i.e. agents, policy managers, etc.) in Gangadharan, therefore, is concerned with security policy propagation, while the claimed invention communicates the actual intrusion attempt (i.e. offending packet or message).

While the Office Action seems to suggest an analogy between the claimed IPC intercept/external data security device and the Gangadharan gateway firewall/micro firewalls, the Gangadharan approach equips each of these to handle intrusions autonomously (p. 330, sec. 5), while in contrast the present invention redirects potential intrusions to a common access point via an IPC (interprocess communication) interception for processing by a data security device (page 10, lines 20-22). A further aspect of this approach not shown or disclosed in Gangadharan, Krack '369 or Balasubramaniyan is mitigation of the overhead required to process the detected intrusions. The claimed invention offloads this overhead to an external data security device, thus avoiding performance degradation for processing the intrusion attempts, as discussed at page 6, lines 20-26.

In further clarification and distinction of the above, Claim 1 has been herein amended to recite:

replacing the determined DLL for database access with an interface wrapper, the interface wrapper for identifying the local agent as a responsive entity for database calls such that the interface wrapper spoofs the database access gateway as the entity responsive to database access attempts, the interface wrapper thus defining an IPC intercept for receiving database connection attempts prior to receipt by the database access gateway, as disclosed in the specification as filed at page 17, line 20-page 18, line 6).

Claim 1 further clarifies:

establishing, in response to the identified connection attempt, an event notification list responsive to database access attempts using the identified connection , as recited in the specification at page 18, lines 6-11, and:

storing, in the event notification list, the local agent as the first entity to receive control from a database access attempt via the identified connection, the event notification list operable to initiate handlers responsive to the event, as discussed at page 18, lines 20-24. Gangadharan makes no suggestion of an event notification list, nor of issuing a first notification. The cited portions of Gangadharan teach an intrusion that BYPASSES the gateway firewall, thus resulting in the local micro firewall receiving the first notification of the intrusion, but the selection is among the two firewall entities, not between the intended recipient (i.e. DB) and the protecting entity (i.e. claimed IPC intercept) defined by the DB interface wrapper.

Claim 44 has been herein added to clarify and refine applicant's distinguishing features, reciting further:

determining a dynamic linked library (DLL) responsive to database access requests for transferring control to a database access gateway, as discussed at page 16:23-27 of Applicant's specification as filed;

identifying an attempt to connect to the database, disclosed at page 17:15-16;

identifying an event corresponding to a database access attempt via the identified connection, disclosed at page 20:8-20;

storing the database access attempt in an instruction register in shared memory operable to receive pending database requests, as discussed at page 20:8-10;

publishing the event corresponding to the database access attempt, publishing causing invocation according to the event notification list, as taught at page 20:10-14; and

invoking the local agent responsive to the event notification list, the invoking causing the local agent to copy the database access attempt from the shared memory and forward the database access attempt to the data security device for processing and logging as a database access, as clarified at page 20:25- page 21:10.

Further, one of skill in the art would not look to modify Krack '369 with Gangadharan because Krack teaches network security via secure sockets (Krack, col. 8, lines 37-44, while Gangadharan suggests using distributed agents (p. 330, last paragraph). Further, even if one were to combine Krack with Gangadharan, the claimed invention would still not be realized because both Krack and Gangadharan teach multi-tiered security (Krack, col. 5, lines 30-35, Gangadharan p. 330, sec. 5) as discussed above. Accordingly, there is no showing, teaching, or suggestions, alone or in combination, of Krack, Balasubramaniyan (previously discussed) and Gangadharan of the claimed IPC mechanism defined by a dynamic linked library (DLL), as discussed above along with other distinguishing features of Applicant's invention.

Claims 40 and 41, deemed largely cumulative in coverage, have been herein canceled in the interest of expedition prosecution of the present application. As the remaining claims depend from, either directly or indirectly, from claims 1, 18, 21, 42 and 44, it is respectfully submitted that all claims are now in condition for allowance.

Applicant(s) hereby petition(s) for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,

/CJL/
Christopher J. Lutz, Esq.
Attorney for Applicant(s)
Registration No.: 44,883
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: GRD03-04

Dated: February 19, 2008